УДК 343.98

ОСОБЕННОСТИ ПРОИЗВОДСТВА ОСМОТРА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО ДЕЛАМ О ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ СПЕЦИАЛЬНОГО РАЗРЕШЕНИЯ (ЛИЦЕНЗИИ)

Д. А. Свиридов
Могилевский институт МВД Республики Беларусь,
начальник кафедры уголовного процесса и криминалистики
e-mail: dima.sviridov@inbox.ru

Аннотация. *В статье рассматриваются вопросы производства такого следственного действия, как осмотр, по уголовным делам об осуществлении предпринимательской деятельности без специального разрешения (лицензии). Делается акцент на осмотре компьютерной информации. Предлагаются рекомендации по проведению осмотра компьютерной информации. Предлагается внесение изменений в Уголовно-процессуальный кодекс Республики Беларусь.*

Ключевые слова: *киберпреступность, законодательство, следственное действие, осмотр, предпринимательская деятельность, расследование преступления.*

Annotation. *The article deals with the production of such an investigative action as an inspection in criminal cases on the implementation of entrepreneurial activities without a special permit (license). Emphasis is placed on the examination of computer information. Suggested recommendations for the inspection of computer information. It is proposed to amend the Criminal Procedure Code of the Republic of Belarus.*

Keywords: *cybercrime, legislation, investigative action, examination, entrepreneurial activity, crime investigation.*

Характеризуя преступления в сфере предпринимательской деятельности, совершаемые с использованием компьютерной и иной техники, представляется верным сделать вывод о том, что деяния в данной сфере представляют опасность за счет сложности их раскрытия и высокой латентности. Несмотря на то, что национальный законодатель относит преступление, предусмотренное ст. 233 Уголовного кодекса Республики Беларусь, — предпринимательская деятельность, осуществляемая без специального разрешения (лицензии) — к категории тяжких преступлений (ч. 3), при определенных обстоятельствах такое преступление может перерасти и в категорию особо тяжких, так как зачастую оно идет в совокупности с коррупционными преступлениями (взяточничество, должностные преступления и т. д.) [1].

В связи с вышеуказанными проблемами в настоящее время вопрос, связанный с раскрытием и расследованием преступлений, направленных

на нарушение правил ведения предпринимательской деятельности с использованием компьютерной техники, стоит достаточно остро. В том числе это в полной мере касается и такого следственного действия, как осмотр места происшествия, в частности осмотр компьютерной техники [2, с. 46].

Активное развитие технического прогресса предсказуемо ведет к совершенствованию криминалистической техники, которая используется при производстве различных следственных и иных процессуальных действий. Это в полной мере касается и такого следственного действия, как осмотр. В современных реалиях возникают новые объекты осмотра, среди которых необходимо отметить не только электронные носители информации и средства мобильной связи, но и непосредственно информацию, которая на них содержится. Так, в ст. 204^1 Уголовно-процессуального кодекса Республики Беларусь (далее — УПК) появился такой вид осмотра, как осмотр компьютерной информации. Данный факт предсказуемо повлек за собой необходимость разработки соответствующей методики его производства.

Как известно, помимо фиксации непосредственной обстановки совершения преступления, в качестве основных задач осмотра места происшествия в ходе расследования уголовных дел о предпринимательской деятельности, совершаемой без специального разрешения (лицензии) (впрочем, как и по иным преступлениям с использованием компьютерных и иных технических средств), выступают обнаружение, фиксация и изъятие цифровых следов. Представляется верным согласиться, что при расследовании уголовных дел данной категории качество проведения осмотра компьютерной информации определяет сбор доказательств и расследование преступления в дальнейшем [3, с. 34].

В ходе осмотра в первую очередь следует обращать внимание на то, что описываются установленные цифровые следы, что возможно в процессе изучения содержательной части электронных документов, а не материального носителя. Следует отметить, что специфика следообразования в цифровой среде существенно усложняет получение электронных доказательств, отвечающих требованиям допустимости, относимости и достоверности. Видится необходимым отметить, что термин «электронные доказательства» в последнее время достаточно часто употребляется в юридической литературе. При этом термин «компьютерная информация» также широко используется в научной полемике, в том числе отражен в УПК [4, с. 104]. Чаще всего доказательствами становятся электронные файлы, записи, сообщения, которые хранятся на электронных носителях. Эти объекты будут приобретать процессуальное значение по любым уголовным делам, так как любое обстоятельство, подлежащее доказыванию, возможно представить в цифровой форме.

Проведенное исследование позволило выделить группы следов преступлений, связанных с осуществлением предпринимательской деятельности без специального разрешения (лицензии), выявляемых в ходе осмотра:

– непосредственно материальные следы: компьютерные и иные технические средства, физические носители информации, дополнительное оборудование, следы пальцев рук на указанных объектах;

– цифровые следы, содержащие основную информацию о способе совершения преступления.

Что может выступать в качестве таких следов? Прежде всего к ним следует отнести электронные документы, лог-файлы журналов и отчетов операционной системы, лог-файлы журналов и отчетов иных приложений и программ; файлы программного обеспечения (модификации, сканирования, копирования); электронные данные различных мессенджеров и телекоммуникационных сервисов и др.

В процессе осмотра места происшествия лицу, осуществляющему расследование уголовного дела, прежде всего интересна информация, как правило, хранящаяся на каком-либо материальном носителе информации. Такого рода техническое устройство само по себе, в соответствии с уголовно-процессуальным законодательством, является вещественным доказательством, а компьютерная информация должна приобретать такой вид доказательства, как электронное, основанное на содержании компьютерной информации. В отдельных случаях в ходе осмотра места происшествия может осуществляться копирование компьютерной информации с соблюдением требований ч. 3^1 ст. 204 УПК. В этом случае будет отсутствовать материальный носитель и будет идти речь только об электронном доказательстве.

Осмотр технических устройств и компьютерной информации в большинстве случаев требует наличия специальных знаний и методик. В целом следует отметить, что для успешного производства осмотра таких объектов, несмотря на наличие необходимых специалистов, нужно владеть минимальными знаниями не только в экономической сфере, но и в сфере работы с техническими устройствами и компьютерной информацией, что видится необходимым для определения компетенции для расследования уголовных дел, связанных с осуществлением предпринимательской деятельности, осуществляемой без специального разрешения (лицензии). Выбор конкретной методики производства осмотра будет предопределяться конкретной следственной ситуацией. Вместе с тем в криминалистике при производстве осмотра традиционно выделяют подготовительный, рабочий и заключительный этапы. Соответственно, каждому этапу характерны определенные алгоритмы действий.

В практической деятельности у лица, осуществляющего расследование по уголовному делу, зачастую возникает такая проблема — компьютерная информация может быть труднодоступной по причине ее нахождения на удаленных серверах, в том числе за пределами государства, и доступ к ней может быть ограничен определенными идентификационными данными, получить которые достаточно проблематично, а без специальных знаний невозможно.

В ходе производства осмотра лицо, осуществляющее расследование уголовного дела, не только описывает то, что увидело на мониторе или дисплее, но и в том числе работает с различными каталогами и папками, программным обеспечением, файлами, лог-файлами журналов и отчетов. Кроме того, лицо может осуществлять манипуляции, направленные на совершение диагностических действий, которые, как правило, выполняются специалистами, приглашенными к участию в этом следственном действии. В целом осмотр таких объектов может проводиться лицом, осуществляющим расследование, самостоятельно, что предусмотрено ч. 3 ст. 204^1 УПК, но в практической деятельности такие осмотры проводятся с приглашением соответствующего специалиста, что обусловлено рядом причин. Прежде всего это вызвано тем, что развитие научно-технического прогресса позволяет осуществлять настройку компьютерного устройства таким образом, что любая неосторожная манипуляция может спровоцировать срабатывание установленной защиты данных и последние могут быть уничтожены.

Уголовно-процессуальное законодательство Республики Беларусь позволяет производить действия, которые предусмотрены функционалом информационных систем и ресурсов, использовать научно-технические средства, оборудование и программное обеспечение при условии отражения всех совершенных манипуляций и применяемых средств в протоколе осмотра. Следует отметить, что работа с информацией, содержащейся на компьютерном устройстве, достаточно затратна по времени, в связи с чем лицо, осуществляющее расследование по уголовному делу, зачастую в ходе осмотра осуществляет изъятие технического устройства, отражая данный факт в протоколе, а в последующем назначает соответствующие компьютерно-технические экспертизы. Кроме того, достаточно остро стоит вопрос восстановления удаленной информации, хотя данный вопрос в большинстве случаев решается не самостоятельно лицом, производящим осмотр, а посредством соответствующих экспертиз. Представляется верным самостоятельно не заниматься восстановлением удаленных данных, а зафиксировать в проколе факт изъятия технического устройства, а затем воспользоваться специальными знаниями при производстве экспертизы [5, с. 241].

Также достаточно интересным будет вопрос осмотров облачных сервисов по хранению информации. Облачные хранилища данных представляют собой виртуальную базу потенциальных доказательств при расследовании уголовных дел, так как нередко содержат информацию об обстоятельствах совершенного преступления. Нередко такие облачные хранилища собирают информацию по умолчанию настроек и не удаляются злоумышленниками. Однако доступ к облачному хранилищу, как правило, ограничен.

Таким образом, следует отметить, что компьютерная информация, содержащаяся на различных технических устройствах, виртуальное пространство по делам о предпринимательской деятельности, осуществляемой без специального разрешения (лицензии), являются местом происшествия, осмотр которого следует проводить по тем же принципам и законодательным требованиям, как и иные осмотры. Особенностью осмотра этих объектов является то, что действия необходимо фиксировать, как правило, посредством видеозаписи. Кроме того, следует отметить необходимость совершенствования уголовно-процессуального законодательства Республики Беларусь, которые бы касались придания правового статуса «электронным доказательствам», закрепления положения о необходимости использования помощи специалиста при осмотре компьютерной информации.

1. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : с изм. и доп. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

2. Протасевич А. А., Зверянская Л. П. Криминалистическая характеристика компьютерных преступлений // Рос. следователь. 2013. № 11. С. 45–47. Вернуться к статье

3. Иванов Д. А. Роль участников уголовного судопроизводства в реализации механизма возмещения вреда, причиненного преступлением, в досудебном производстве по уголовным делам // Вестн. Моск. ун-та им. С. Ю. Витте. Сер. 2 : Юрид. науки. 2015. № 1 (6). С. 33–36. Вернуться к статье

4. Свиридов Д. А., Свешников Д. В. К вопросу о понятии «электронное доказательство» [Электронный ресурс] // Актуальные проблемы уголовного процесса и криминалистики : сб. науч. ст. / Могилев. ин-т МВД ; редкол. : Ю. П. Шкаплеров (председ.) [и др.]. Могилев : Могилев. ин-т МВД, 2021. 1 электрон. опт. диск (CD-R). Вернуться к статье

5. Свешников Д. В., Шилко Ж. А. Актуальность совершенствования отдельных уголовно-процессуальных и уголовных норм в сфере противодействия киберпреступности [Электронный ресурс] // Правовая культура в современном обществе : сб. науч. ст. / Могилев. ин-т МВД ; редкол. : И. А. Демидова (отв. ред.) [и др.]. Могилев : Могилев. ин-т МВД, 2021. 1 электрон. опт. диск (CD-R). Вернуться к статье